



Norton  
**AntiVirus**<sup>TM</sup> 9.0  
For Macintosh®

## User's Guide

# Norton AntiVirus™ for Macintosh®

## User's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 9.0

PN: 10067169

### Copyright Notice

Copyright © 2003 Symantec Corporation. All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

### Trademarks

Symantec, the Symantec logo, Norton AntiVirus, and LiveUpdate are U.S registered trademarks of Symantec Corporation. Symantec Security Response is a trademark of Symantec Corporation.

Mac, Macintosh, Mac OS, and the Mac logo are trademarks of Apple Computer, Inc. Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

# Symantec License and Warranty

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL. MAKE NO FURTHER USE OF THE SOFTWARE, AND RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY (60) DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

## 1. License:

The software which accompanies this license (collectively the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that Symantec may furnish to you. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") which accompanies, precedes, or follows this license, your rights and obligations with respect to the use of this Software are as follows:

### You may:

- A. use one copy of the Software on a single computer. If a License Module accompanies, precedes, or follows this license, you may make that number of copies of the Software licensed to you by Symantec as provided in your License Module. Your License Module shall constitute proof of your right to make such copies.
- B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of your computer and retain the original for archival purposes;
- C. use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network; and
- D. after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this license.

### You may not:

- A. copy the printed documentation which accompanies the Software;
- B. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
- C. use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;
- D. use a later version of the Software than is provided herewith unless you have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;
- E. use, if you received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which you have not received a permission in a License Module; or
- F. use the Software in any manner not authorized by this license.

## 2. Content Updates:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which you have purchased a subscription for Content Updates for the Software (including any subscription included with your original purchase of the Software), purchased upgrade insurance for the Software, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit you to obtain and use Content Updates.

## 3. Sixty Day Money Back Guarantee:

If you are the original licensee of this copy of the Software and are dissatisfied with it for any reason, you may return the complete product, together with your receipt, to Symantec or an authorized dealer, postage prepaid, for a full refund at any time during the sixty (60) day period following the delivery to you of the Software.

## 4. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements

or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

## 5. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

## 6. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

## 7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement may only be modified by a License Module or by a written document which has been signed by both You and Symantec. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, USA, or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

# Contents

|                  |  |    |
|------------------|--|----|
| <b>Chapter 1</b> | <b>About Norton AntiVirus for Macintosh</b>            |    |
|                  | What's new in Norton AntiVirus .....                   | 9  |
|                  | How viruses work .....                                 | 10 |
|                  | Macro viruses spread quickly .....                     | 10 |
|                  | Trojan horses hide their true purposes .....           | 10 |
|                  | Worms take up space .....                              | 11 |
|                  | How viruses spread .....                               | 11 |
|                  | How Norton AntiVirus works .....                       | 12 |
|                  | The virus definition service stops known viruses ..... | 12 |
|                  | Bloodhound technology stops unknown viruses .....      | 12 |
|                  | Auto-Protect keeps you safe .....                      | 12 |
|                  | Is my computer protected now? .....                    | 12 |
|                  | How to maintain protection .....                       | 13 |
|                  | Avoid viruses .....                                    | 13 |
|                  | Prepare for emergencies .....                          | 13 |
| <b>Chapter 2</b> | <b>Installing Norton AntiVirus</b>                     |    |
|                  | System requirements .....                              | 15 |
|                  | Before installation .....                              | 16 |
|                  | Read the Read Me file .....                            | 16 |
|                  | Installation .....                                     | 16 |
|                  | Restart your computer .....                            | 19 |

|   |    |
|---|----|
| After installation .....                                    | 20 |
| If you can't eject the CD .....                             | 20 |
| Register Norton AntiVirus .....                             | 20 |
| Read Late Breaking News .....                               | 22 |
| If you connect to the Internet through America Online ..... | 22 |
| Explore the CD .....  | 23 |
| If you need to uninstall Norton AntiVirus .....             | 23 |

## Chapter 3    **Norton AntiVirus basics**

|   |    |
|---|----|
| How to start and exit Norton AntiVirus .....                    | 25 |
| Enable and disable Norton AntiVirus Auto-Protect .....          | 26 |
| Disable Auto-Protect temporarily .....                          | 27 |
| For more information .....                                      | 27 |
| Access Help .....   | 27 |
| Access the User's Guide PDF .....                               | 28 |
| Open the Read Me file .....                                     | 28 |
| Explore the Symantec support Web site .....                     | 29 |
| Subscribe to the Symantec Security Response<br>newsletter ..... | 30 |

## Chapter 4    **Protecting against new threats**

|  |    |
|--|----|
| About program updates .....                      | 31 |
| About protection updates .....                   | 32 |
| About your subscription .....                    | 32 |
| When you should update .....                     | 32 |
| Before updating .....                            | 32 |
| If you use America Online to connect .....       | 33 |
| If you update on an internal network .....       | 33 |
| If you can't use LiveUpdate .....                | 33 |
| Update procedures .....                          | 34 |
| Update everything now .....                      | 35 |
| Customize a LiveUpdate session .....             | 35 |
| After updating .....                             | 35 |
| View the LiveUpdate Summary .....                | 35 |
| Empty the Trash after a LiveUpdate session ..... | 36 |
| Check product version numbers and dates .....    | 36 |
| Schedule future updates .....                    | 36 |

## Chapter 5    **Scheduling future events**

|                                  |    |
|----------------------------------|----|
| About Norton Scheduler .....     | 37 |
| Open Norton Scheduler .....      | 37 |
| Schedule LiveUpdate events ..... | 38 |

|   |    |
|---|----|
| Schedule Norton AntiVirus scans .....     | 39 |
| Select an item for a scheduled scan ..... | 40 |
| Set a start time .....                    | 40 |
| Manage scheduled events .....             | 40 |
| Edit scheduled events .....               | 40 |
| Delete scheduled events .....             | 41 |
| Disable scheduled events .....            | 41 |
| Reset scheduled tasks .....               | 41 |

## Chapter 6 Protecting disks, files, and data from viruses

|  |    |
|--|----|
| Scan disks, folders, and files .....       | 43 |
| If problems are found during a scan .....  | 45 |
| Scan email attachments .....               | 45 |
| Scan and repair in archives .....          | 45 |
| View and print scan history .....          | 46 |
| Save and print scan reports .....          | 46 |
| Perform a scan from the command line ..... | 47 |

## Chapter 7 What to do if a virus is found

|   |    |
|---|----|
| Auto-Protect finds a virus .....                              | 49 |
| Auto-Protect finds a virus and repairs the file .....         | 50 |
| Auto-Protect finds a virus but does not repair the file ..... | 50 |
| Auto-Protect finds a virus and cannot repair the file .....   | 51 |
| A virus is found when removable media is inserted .....       | 51 |
| Repair, Delete, and Restore in Quarantine .....               | 51 |
| A virus is found during a user-initiated scan .....           | 52 |
| Repair infected files .....                                   | 52 |
| If Norton AntiVirus can't repair a file .....                 | 53 |
| If removable media is infected .....                          | 53 |
| Look up virus names and definitions .....                     | 53 |
| Look up virus definitions on the Symantec Web site .....      | 54 |

## Chapter 8 Customizing Norton AntiVirus

|                                      |    |
|--------------------------------------|----|
| About Auto-Protect Preferences ..... | 55 |
| Set Auto-Protect Preferences .....   | 56 |
| About User Preferences .....         | 56 |
| Set Scan Preferences .....           | 57 |
| Set Repair Preferences .....         | 57 |
| Set a Reminder .....                 | 58 |
| Customize the Norton QuickMenu ..... | 58 |

**Chapter 9    Troubleshooting in Norton AntiVirus**

|   |    |
|---|----|
| Installation problems .....   | 59 |
| I can't install Norton AntiVirus .....  | 59 |
| Startup problems .....  | 59 |
| Norton AntiVirus Auto-Protect fails to load when I<br>start my Macintosh .....                        | 60 |
| Norton AntiVirus reports that a file is invalid when<br>trying to launch or scan, or at startup ..... | 60 |
| Norton AntiVirus cannot find the Norton AntiVirus<br>virus definitions file .....                     | 60 |
| Why can't I create an alias to Norton AntiVirus? .....  | 60 |
| Protection problems .....   | 61 |
| Scanning and account access privileges .....  | 61 |
| I need to rescan files that have already been scanned .....   | 61 |
| I'm having trouble updating virus definitions using<br>LiveUpdate .....                               | 62 |
| Other troubleshooting steps .....   | 62 |
| Error messages .....  | 62 |
| Auto-Protect error message .....  | 63 |
| Password and administrator messages .....   | 63 |

**Appendix A    Using Norton AntiVirus on a network**

|  |    |
|--|----|
| Notes to the administrator .....           | 65 |
| Scanning network drives .....              | 65 |
| Preparing an emergency response plan ..... | 66 |
| Before a virus is detected .....           | 66 |
| If a virus is detected .....               | 67 |

**Service and support solutions**

**Glossary**

**Index**

**CD Replacement Form**



# About Norton AntiVirus for Macintosh



Whenever you send and receive email, insert a CD or floppy disk, open an email attachment, or download a program from a news group or Web site, you risk receiving a virus. Norton AntiVirus for Macintosh provides comprehensive virus prevention, detection, and elimination for your computer. It finds and repairs infected files (files that contain viruses) to keep your data safe and secure.

## What's new in Norton AntiVirus

Version 9.0 of Norton AntiVirus for Macintosh now includes:

- Complete antivirus protection of both Mac OS X 10.1.5 and Mac OS 8.1 to 9.x in one version
- Quarantine of infected files that cannot be repaired
- Scan on mount of removable disks including CD, Zip, and floppy which further extends the security of your data
- Tool drawer which allows customized and maximized access to your antivirus tools
- The Norton QuickMenu from which you can modify Auto-Protect
- Identification and repair of Windows and DOS viruses in files and archives so hidden PC viruses cannot be planted in your computer and spread to Windows computers
- Scan and repair of files inside archives, excluding Stuffit, without user prompt

## How viruses work

A computer virus is a parasitic program written intentionally to alter the way your computer operates without your permission or knowledge. A virus attaches copies of itself to other files and, when activated, may damage files, cause erratic system behavior, or display messages.

Computer viruses infect System files, or files stored in the System folder that the Macintosh computer uses to start up and documents created by programs with macro capabilities. Mac OS System files include kernel extensions (programs that load into memory when a Macintosh computer is started), and programs like those in Microsoft Office.

Some computer viruses are programmed specifically to corrupt programs, delete files, or erase your disk.

### Macro viruses spread quickly

Macros are simple programs that are used to do things such as automate repetitive tasks in a document or make calculations in a spreadsheet. Macros are written in files created by such programs as Microsoft Word and Microsoft Excel.

Macro viruses are malicious macro programs that are designed to replicate themselves from file to file and can often destroy or change data. Macro viruses can be transferred across platforms and spread whenever you open an infected file.

### Trojan horses hide their true purposes

*Trojan horses* are programs that appear to serve some useful purpose or provide entertainment, which encourages you to run them. But the program also serves a covert purpose, which may be to damage files or place a virus on your computer.

A Trojan horse is not a virus because it does not replicate and spread like a virus. Because Trojan horses are not viruses, files that contain them cannot be repaired. To ensure the safety of your computer, Norton AntiVirus detects Trojan horses so you can delete them from your computer.

## Worms take up space

Worms are programs that replicate without infecting other programs. Some worms spread by copying themselves from disk to disk. They search for specific types of files on a hard disk and try to damage or destroy those files. Other worms replicate only in memory, creating myriad copies of themselves, all running simultaneously, which slows down the computer. Like *Trojan horses*, worms are not viruses and therefore cannot be repaired. They must be deleted from your computer.

## How viruses spread

A virus is inactive until you launch an infected program, start your computer from a disk that has infected system files, or open an infected document. For example, if a word processing program contains a virus, the virus activates when you run the program. Once a virus is in memory, it usually infects any program you run, including network programs (if you can make changes to network folders or disks).

Viruses behave in different ways. Some viruses stay active in memory until you turn off your computer. Other viruses stay active only as long as the infected program is running. Turning off your computer or exiting the program removes the virus from memory, but does not remove the virus from the infected file or disk. That is, if the virus resides in an operating system file, the virus activates the next time you start your computer from the infected disk. If the virus resides in a program, the virus activates the next time you run the program.

To prevent virus-infected programs from getting onto your computer, scan files with Norton AntiVirus before you copy or run them. This includes programs you download from news groups or Internet Web sites and any email attachments that you receive.

Macintosh computers that are attached to multiplatform networks can potentially be affected by Windows-based viruses. If you store Macintosh files on network servers accessible by Windows-based computers, those files could potentially be attacked by Windows viruses or *worms* programmed to damage files.

## How Norton AntiVirus works

Norton AntiVirus monitors your computer for known and unknown viruses. A known virus is one that can be detected and identified by name. An unknown virus is one for which Norton AntiVirus does not yet have a definition.

Norton AntiVirus protects your computer from both types of viruses, using *virus definitions* to detect known viruses and Bloodhound technology to detect unknown viruses. Virus definitions and Bloodhound technology are used during scheduled scans and manual scans, and are used by Auto-Protect to constantly monitor your computer.

### The virus definition service stops known viruses

See “Look up virus definitions on the Symantec Web site” on page 54.

The virus definition service consists of files that Norton AntiVirus uses to recognize viruses and intercept their activity. You can look up virus names in Norton AntiVirus and access an encyclopedia of virus descriptions on the Symantec Web site.

### Bloodhound technology stops unknown viruses

Bloodhound is the Norton AntiVirus scanning technology for detecting new and unknown viruses. It detects viruses by analyzing an *executable file's* structure, behavior, and other attributes such as programming logic, computer instructions, and any data contained in the file.

### Auto-Protect keeps you safe

Norton AntiVirus Auto-Protect loads into memory when your computer starts up, and provides constant protection while you work. It eliminates viruses and Trojan horses, including macro viruses, and quarantines and repairs damaged files. It also checks for viruses every time you use software programs on your computer, insert floppy disks or other *removable media*, use the Internet, or copy or save files to your computer.

## Is my computer protected now?

Once you have installed Norton AntiVirus and restarted your computer, you are safe from viruses. To ensure protection, leave Auto-Protect on so that Norton AntiVirus automatically finds viruses. Use LiveUpdate to protect against new viruses.

## How to maintain protection

When Norton AntiVirus is installed, you have complete virus protection. However, new viruses are created constantly. Viruses can spread when you start your computer from an infected disk or when you run an infected program. There are several things you can do to avoid viruses and to recover quickly should a virus strike.

### Avoid viruses

It is important that you practice regular file maintenance and that you keep Norton AntiVirus up-to-date.

To avoid viruses:

- Stay informed about viruses by logging on to the Symantec Security Response Web site (<http://securityresponse.symantec.com>) where there is extensive, frequently updated information on viruses and virus protection.
- Use LiveUpdate regularly to update your programs and virus definition service files.
- Keep Norton AntiVirus Auto-Protect turned on at all times to prevent viruses from infecting your computer.
- Schedule scans to occur automatically.

See "Protecting against new threats" on page 31.

### Prepare for emergencies

It is important that you are prepared in case your computer is infected by a virus. To prepare for emergencies back up files regularly and keep more than just the most recent backup.



# Installing Norton AntiVirus

# 2

Before installing Norton AntiVirus, take a moment to review the system requirements.

Files from previous versions of Norton AntiVirus and Symantec AntiVirus for Macintosh are deleted when you install Norton AntiVirus to the same location.



Versions of Norton AntiVirus for both Mac OS 8.1 to 9.x and Mac OS X are included on the CD. For instructions on installing and using Norton AntiVirus for Mac OS 8.1 to 9.x, see the *Norton AntiVirus User's Guide* PDF in the Install for OS 9 folder on the CD.

## System requirements

Norton AntiVirus does not support Mac OS X versions 10.0 to 10.1.4. If you want to install Norton AntiVirus on Mac OS X, you must upgrade to Mac OS X 10.1.5.

- Macintosh OS X version 10.1.5 or later
- G3 or G4 processor
- 128 MB of RAM
- 30 MB of available hard disk space for installation
- Internet connection (recommended)
- CD-ROM or DVD-ROM drive

## Before installation

The Read Me file on the Norton AntiVirus for Macintosh CD contains late-breaking information and installation troubleshooting tips, which you should read before you install Norton AntiVirus.

### Read the Read Me file

The Read Me file contains a summary of what's new and changed in Norton AntiVirus, along with condensed versions of key procedures and technical tips. In addition, see the Read Me file for late-breaking information and installation troubleshooting tips.

#### To read the Read Me file

- 1 Insert the Norton AntiVirus for Macintosh CD into your CD-ROM drive.
- 2 In the CD window, open the **Install for OS X** folder.
- 3 Double-click the **Read Me** file.

## Installation

Install Norton AntiVirus from the Norton AntiVirus for Macintosh CD.



Norton AntiVirus protects both Mac OS X and Classic.

The install procedure requires that you enter an Administrator password. If you do not know if your login is an Admin login, you can check it in System Preferences.

#### To check your login type

- 1 On the Apple menu, click **System Preferences**.
- 2 Do one of the following:
  - In Mac OS X, version 2 and later, click **Accounts**.
  - In Mac OS X, version 10.1.5, click **Users**.Your login name and type are listed.

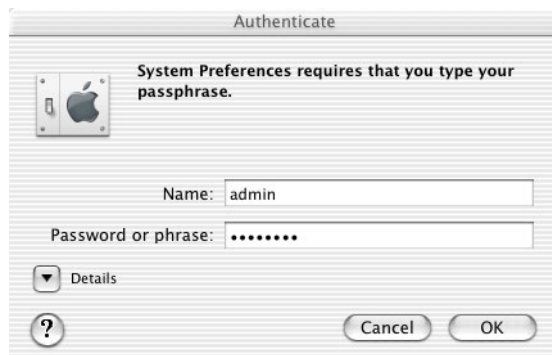


### To install Norton AntiVirus for Macintosh

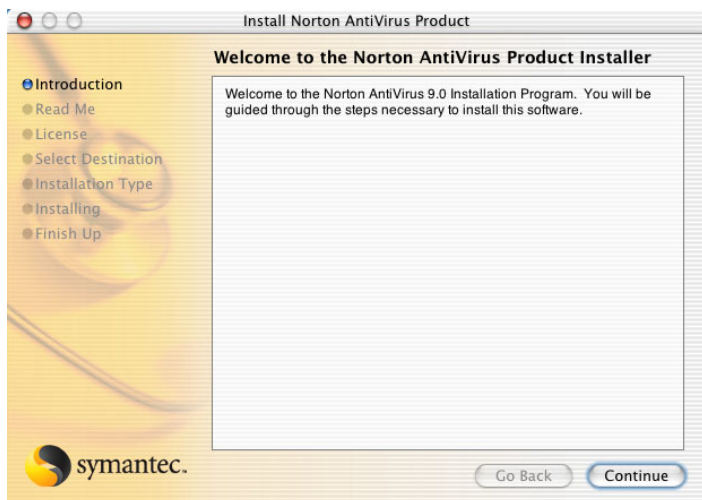
- 1 Insert the Norton AntiVirus for Macintosh CD into the CD-ROM drive. If the CD window doesn't open automatically, double-click the CD icon to open it.
- 2 In the CD window, open the **Install for OS X** folder.
- 3 Double-click **Norton AntiVirus Installer**.



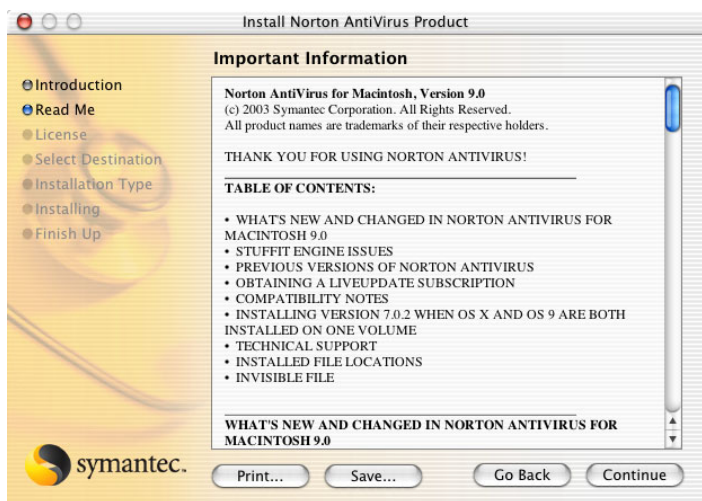
If you are installing Norton AntiVirus on Mac OS X 10.1.5, the Authenticate window does not automatically appear. Click the lock in the lower-left corner of the Authorization window to open the Authenticate window and continue with the rest of the procedure.



- 4 In the Authenticate window, type your Administrator password, then click **OK**.

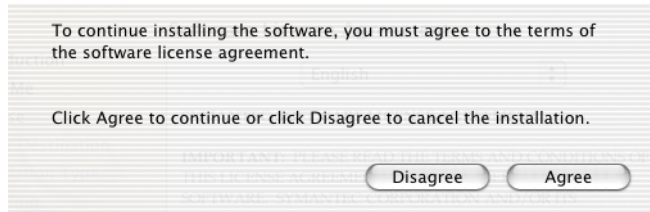


- 5 In the Welcome to the Norton AntiVirus Product Installer window, click **Continue**.



- 6 Review the Read Me text, then click **Continue**.

- 7 In the Software License Agreement window, click **Continue**.



- 8 In the agreement dialog box that appears, click **Agree**.  
If you disagree, you cannot continue with the installation.
- 9 In the Select a Destination window, select the disk on which you want to install Norton AntiVirus, then click **Continue**.
- 10 In the Easy Install window, click **Install**.  
If you have other Symantec products installed on your computer, this button may say Upgrade.
- 11 Choose whether or not you want to run LiveUpdate to ensure your software is up-to-date.
- 12 When installation is complete, click **Restart**.

## Restart your computer

After you install Norton AntiVirus and restart your computer, it is protected from viruses. Norton Auto-Protect loads each time that you start your computer and actively protects your computer unless you disable it.

# After installation

Now that you’ve installed and restarted Norton AntiVirus, you have the following options:

| Task  | More information  |
|---|---|
| Register your software.   | See <a href="#">“Register Norton AntiVirus”</a> on page 20. |
| Check for late-breaking news about your new software. Use the Internet link installed in the Norton AntiVirus folder. | See <a href="#">“Read Late Breaking News”</a> on page 22.   |
| Explore the additional features and programs included on the CD.  | See <a href="#">“Explore the CD”</a> on page 23.            |

## If you can’t eject the CD

If you have trouble ejecting the CD after you restart your computer, try one of the following:

- Press the CD-ROM drive’s eject button when your Macintosh restart chime sounds.
- On a newer Macintosh computer with a slot-loading CD-ROM drive, press the mouse button while starting up to eject the CD.

When you install Norton AntiVirus and leave default settings, you are protected from most viruses after you restart.

## Register Norton AntiVirus

Using your existing Internet connection, you can register Norton AntiVirus for Macintosh via the Internet (the global network of computers).

## To register Norton AntiVirus via the Internet

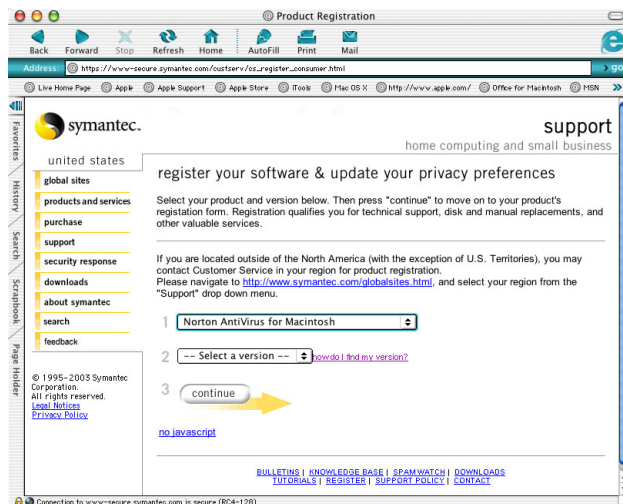
- 1 Connect to the Internet.  
If you use America Online (AOL) to connect to the Internet, you need to connect to it first. See [“To connect to the Symantec Web site via AOL”](#) on page 22.
- 2 In the Norton Solutions folder, double-click **Register Your Software**.



Register Your Software

Your default Internet browser displays the Symantec Service & Support registration page.

- 3 On the support page, click **I am a home/small business user**.



- 4 On the register your software page, click **Norton AntiVirus for Macintosh**.
- 5 Select the correct version of the product.
- 6 Click **continue**.

## Read Late Breaking News

Norton AntiVirus installs a Late Breaking News link. This link lets you see the latest information for your installed software.

### To read Late Breaking News

- 1 Connect to the Internet.  
If you use America Online (AOL) to connect to the Internet, see [“To connect to the Symantec Web site via AOL”](#) on page 22.
- 2 In the Norton AntiVirus folder, double-click **Late Breaking News**.



Late Breaking News

Your default Internet browser displays the Symantec Late Breaking News Web page for your product.

## If you connect to the Internet through America Online

If you use America Online (AOL) as your Internet service provider (ISP), you must connect to AOL before you go to the Symantec software registration page or view Late Breaking News.

### To connect to the Symantec Web site via AOL

- 1 Log on to AOL.
- 2 On the AOL Welcome page, click the AOL Internet browser.
- 3 Move the AOL browser and any other open AOL windows out of the way.
- 4 In the Norton AntiVirus window, do one of the following:
  - Double-click **Register Your Software**.  
Continue with the registration procedure. See [“Register Norton AntiVirus”](#) on page 20.
  - Double-click **Late Breaking News**.  
Continue with the procedure for reading the news. See [“Read Late Breaking News”](#) on page 22.
- 5 Disconnect from AOL.

## Explore the CD

In addition to the Norton AntiVirus installer folders and program software, there are several other items on the CD:

|                         |   |
|-------------------------|---|
| Documentation folder    | Contains this User's Guide in PDF format and installation files for Adobe Acrobat Reader.   |
| Norton Solutions folder | Contains the LiveUpdate files. Use LiveUpdate to update your installed virus program files and obtain the latest virus definitions. |

## If you need to uninstall Norton AntiVirus

If you need to remove Norton AntiVirus from your computer, use the Symantec Uninstaller on the Norton AntiVirus for Macintosh CD. The process is faster if all other programs are closed before you uninstall Norton AntiVirus.

The uninstall procedure requires that you enter an Administrator password. If you do not know if your login is an Admin login, you can check it in System Preferences.

### To check your login type

- 1 On the Apple menu, click **System Preferences**.
- 2 Click **Accounts**.  
Your login name and type are listed.

**To uninstall Norton AntiVirus**

- 1** Insert the Norton AntiVirus for Macintosh CD into the CD-ROM drive. If the CD window doesn't open automatically, double-click the CD icon to open it.
- 2** In the CD window, open the **Install for OS X** folder.
- 3** Double-click **Symantec Uninstaller**.
- 4** In the Uninstall Symantec Products window, check **Norton AntiVirus**.
- 5** Click **Uninstall**.
- 6** Click **Uninstall** again to confirm that you want to delete the product.
- 7** In the Authenticate window, type your Administrator password, then click **OK**.
- 8** In the window that displays the list of deleted items, click **Close**.
- 9** In the Uninstall Symantec Products window, click **Quit**.



# Norton AntiVirus basics

# 3

Norton AntiVirus basics include general information about how to work with Norton AntiVirus and how to access more information about Norton AntiVirus.

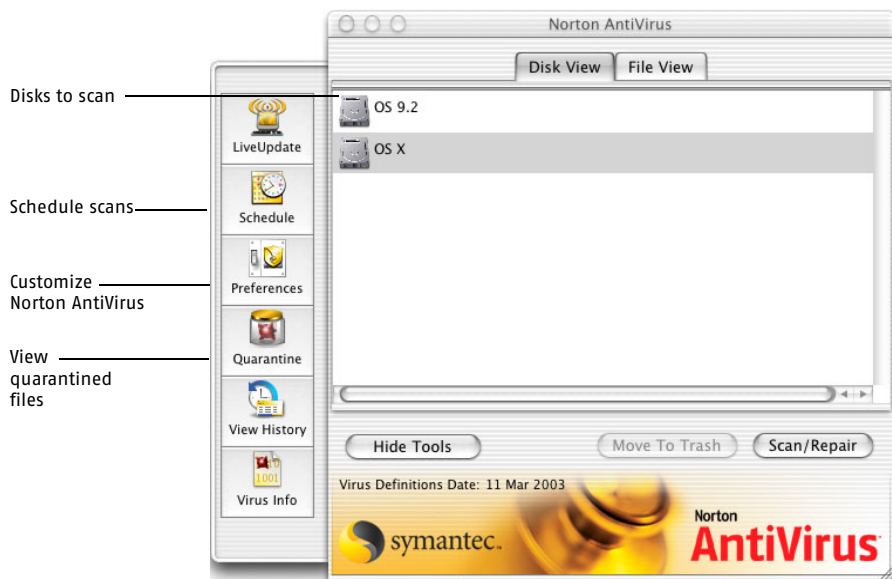
## How to start and exit Norton AntiVirus

You don't have to start the Norton AntiVirus program to be protected from viruses if you have Auto-Protect running. You do have to start Norton AntiVirus when you want to:

- Run manual scans of your computer.
- Schedule Norton AntiVirus to run unattended scans.
- Customize virus protection options.

### To start Norton AntiVirus

- 1 Open the **Norton Solutions** folder.
- 2 Double-click **Norton AntiVirus**.



### To exit Norton AntiVirus

- ❖ Do one of the following:
  - On the Norton AntiVirus menu, click **Quit Norton AntiVirus**.
  - Press **Command-Q**.

## Enable and disable Norton AntiVirus Auto-Protect

By default, Norton AntiVirus Auto-Protect guards against viruses as soon as your computer starts. It checks programs for viruses as they are run and monitors your computer for any activity that might indicate the presence of a virus. Running a Norton AntiVirus manual scan is not necessary as long as Auto-Protect is left on. Auto-Protect interception prevents viruses from moving to your disk.

## Disable Auto-Protect temporarily

To install some programs, you may need to turn off Auto-Protect.

See [“Customize the Norton QuickMenu”](#) on page 58.

### To disable Auto-Protect temporarily

- ❖ On the Norton QuickMenu, click **Norton Auto-Protect > Turn Auto-Protect Off**.

## For more information

Norton AntiVirus provides instructional material in three formats:

|               |   |
|---------------|---|
| User's Guide  | The User's Guide provides basic conceptual information and procedures for using all of the features of Norton AntiVirus. Use the printed User's Guide if you cannot access the online material for any reason. Technical terms that are italicized in the User's Guide are defined in the glossary, which is available in both the User's Guide PDF and Help. |
| Built-in Help | Help includes all the material contained in the User's Guide, plus expanded conceptual information, procedural details, and a glossary for definitions of technical terms. Use Help to answer questions while you are using Norton AntiVirus. See <a href="#">“Access Help”</a> on page 27.   |
| PDF           | The PDF is an electronic version of the User's Guide that you can use if you prefer to look for information online in a book-like format or if you want to provide additional copies of the User's Guide. The PDF also includes a glossary for definitions of technical terms. See <a href="#">“Access the User's Guide PDF”</a> on page 28.                  |

In addition to this material, there is a Read Me file on the Norton AntiVirus for Macintosh CD. Check the Read Me file before you install Norton AntiVirus for late-breaking information.

Finally, you can always check the Symantec Web site for information about Norton AntiVirus. You can also use the Web site to subscribe to the Symantec Security Response newsletter, which provides you with the latest information about viruses and other threats and antithreat technology.

## Access Help

Opening Help in Norton AntiVirus displays the Apple Help Viewer with a list of Help topics.

### To access Help

- ❖ On the Help menu, click **Norton AntiVirus Help**.

Tips for exploring Help:

- To search for a specific topic, in the search field at the top of the Help window, type the related term, then click Ask.
- Terms that are underlined and blue in the text are defined in the glossary. Click the word to go to its definition. Click the left-arrow button to return to the topic.
- Links to related topics appear at the end of a topic.
- Some topics include links that open the window in which you can begin the task described.

## Access the User's Guide PDF

The User's Guide is available in printable Adobe Acrobat PDF format on the CD.

### To open the PDF

- 1 Insert the Norton AntiVirus for Macintosh CD into the CD-ROM drive.
- 2 In the CD window, double-click the **Install for OS X** folder.
- 3 In the Install for OS X folder, double-click the **Documentation** folder.
- 4 Double-click the **Norton AntiVirus User Guide** PDF.

You can also drag the PDF to your hard disk.

Tips for exploring the PDF:

- When you open the PDF, the table of contents appears in the left margin. In the table of contents, click a heading to jump to that topic.
- To search for a specific topic, use the Find command on the Edit menu.
- Terms that are italicized and blue in the text are defined in the glossary. Click the word to go to its definition. Click Go to Previous View to return to the topic.

## Open the Read Me file

The Read Me file on the Norton AntiVirus for Macintosh CD contains information that was unavailable at the time that the User's Guide was published. A single Read Me file contains information for both the Mac OS 8.1 to 9.x and Mac OS X versions of Norton AntiVirus.

**To open the Read Me file**

- 1 Insert the Norton AntiVirus for Macintosh CD into your CD-ROM drive.
- 2 In the CD window, open the **Install for OS X** folder.
- 3 Double-click the **Read Me** file.

## Explore the Symantec support Web site

The Symantec support Web site provides extensive information about Norton AntiVirus. You can find updates, patches, Knowledge Base articles, and virus removal tools.

**To explore the Symantec support Web site**

- 1 On the Internet, go to [www.symantec.com/techsupp](http://www.symantec.com/techsupp)
- 2 On the support Web page, under home/small business, click **continue**.
- 3 On the home computing and small business Web page, click **start online support**.
- 4 Follow the instructions on the Web site to get the information you need.

If you cannot find what you are looking for using the online support pages, try searching the Web site.

**To search the Symantec support Web site**

- 1 On the left side of any Web page in the Symantec support Web site, click **search**.
- 2 Type a word or phrase that best represents the information for which you are looking.  
For tips on entering your search text, click **help** at the bottom of the page.
- 3 Check the area of the Web site that you want to search.
- 4 Click **search**.

## Subscribe to the Symantec Security Response newsletter

Each month, Symantec publishes a free electronic newsletter that is focused on the needs of Internet security customers. It discusses the latest antivirus technology produced by Symantec Security Response, common viruses, trends in virus workings, virus outbreak warnings, and special virus definition releases.

### To subscribe to the Symantec Security Response newsletter

- 1 On the Internet, go to [securityresponse.symantec.com](http://securityresponse.symantec.com)
- 2 On the security response Web page, scroll down to the reference area of the page, then click **Newsletter**.
- 3 On the security response newsletter Web page, select the language in which you want to receive the newsletter.
- 4 Under Subscribe, type the information requested, then click **Subscribe**.

# Protecting against new threats

# 4

When you first install your Symantec product and run LiveUpdate, you have the most current versions of the product and any protection-related files, such as the inappropriate Web site list for Norton Internet Security or the *virus definitions* list for Norton AntiVirus.

At any time, new *threats* can be introduced. Also, some operating system updates may necessitate changes to a program. When these events occur, Symantec provides new files to address these issues. You can get these new files by using LiveUpdate.

Using your existing Internet connection, LiveUpdate connects to the Symantec LiveUpdate server, checks for available updates, then *downloads* and installs them.

## About program updates

Program updates are minor improvements to your installed product, usually available for *download* from a Web site. These differ from product upgrades, which are newer versions of entire products. Program updates that replace sections of existing software are called patches. Patches are usually created to ensure the compatibility of a program with new versions of operating systems or hardware, adjust a performance issue, or fix bugs.

LiveUpdate automates the process of downloading and installing program updates. It locates and downloads files from an Internet site, then installs them, and deletes the leftover files from your computer.

# About protection updates

Protection updates are files available from Symantec by subscription, that keep your Symantec products up-to-date with the latest antithreat technology. The protection updates you receive depend on which products you are using.

|                                      |   |
|--------------------------------------|---|
| Norton AntiVirus, Norton SystemWorks | Users of Norton AntiVirus and Norton SystemWorks receive virus definition service updates, which provide access to the latest virus signatures and other technology from Symantec.  |
| Norton Internet Security             | In addition to the virus definition service, users of Norton Internet Security receive protection updates to the lists of Web site addresses and Web site categories that are used to identify inappropriate Web content. |

# About your subscription

See “Subscription policy” on page 70.

If your Symantec product includes protection updates, the purchase of that product includes a complimentary, limited-time subscription to the updates that are used by your product. When the subscription is due to expire, you are prompted to renew your subscription.

If you do not renew your subscription, you can still use LiveUpdate to obtain program updates. However, you cannot obtain protection updates and will not be protected against newly discovered threats.

# When you should update

See “Schedule future updates” on page 36.

During installation of your software, you have the option to run LiveUpdate. You should do so to ensure that you have the most up-to-date protection files. After installation, if you have Norton AntiVirus, Norton Personal Firewall, Norton Internet Security, or Norton SystemWorks installed, update at least once a month to ensure that you have the latest virus definitions and firewall protection.

# Before updating

In some cases there are preparations you must make before running LiveUpdate. For example, if you use America Online (AOL) as your Internet service provider (ISP), you must log on to AOL before you use LiveUpdate.



## If you use America Online to connect

If you use America Online (AOL) as your *Internet service provider* (ISP), you need to log on to AOL before you use LiveUpdate.

### To use LiveUpdate with AOL

- 1 Log on to AOL.
- 2 On the AOL Welcome page, click the AOL Internet browser.
- 3 Open LiveUpdate.
- 4 Follow the instructions in “Update procedures” on page 34.
- 5 When the LiveUpdate session is complete, close your AOL browser.  
If your LiveUpdate session requires that you restart your computer, disconnect from AOL before restarting.

## If you update on an internal network

If you run LiveUpdate on a Macintosh that is connected to a network that is within a company firewall, your network administrator might set up an internal LiveUpdate server on your network. Once your administrator has configured it, LiveUpdate should find this location automatically.

If you have trouble connecting to an internal LiveUpdate server, contact your network administrator.

## If you can't use LiveUpdate

When new updates become available, Symantec posts them on the Symantec Web site. If you can't run LiveUpdate, you can obtain new update files from the Symantec Web site.



Your subscription must be current to obtain new protection updates from the Symantec Web site.

### To obtain virus definitions from the Symantec Web site

- 1 Start your Internet browser and go to the following site:  
[securityresponse.symantec.com/avcenter/defs.download.html](http://securityresponse.symantec.com/avcenter/defs.download.html)  
If this page doesn't load, go to [securityresponse.symantec.com](http://securityresponse.symantec.com) and click **Download Virus Definitions**, then click **Download Virus Definitions (Intelligent Updater Only)**.
- 2 On the security response page, select **Norton AntiVirus for Macintosh**.

- 3 Click **Download Updates**.
- 4 On the security response page, select the file to download.  
Be sure to select files for the appropriate version of your product.  
Information about the update is included with the download.

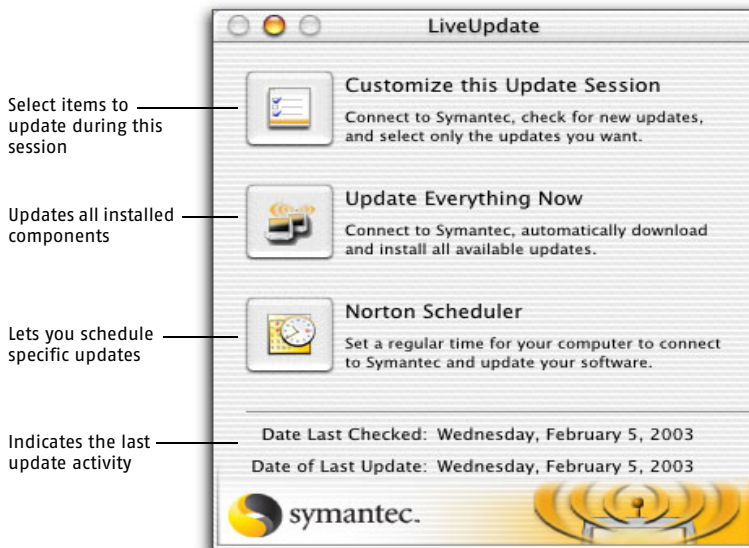
### To obtain product updates from the Symantec Web site

- 1 Open your Internet browser and go to the following site:  
[securityresponse.symantec.com/downloads/](http://securityresponse.symantec.com/downloads/)
- 2 On the downloads page, in the product updates list, select the product for which you want an update.
- 3 On the support page, select the version of the product.
- 4 Click **continue**.
- 5 On the product page, select the file to download.  
Information about the update is included with the download.

## Update procedures

See "[Schedule future updates](#)" on page 36.

You can have LiveUpdate look for all updates at once, or select individual items to update. You can also schedule a future LiveUpdate session.



## Update everything now

Updating all available files is the fastest method to ensure the latest protection for all your Symantec products.

### To update everything now

- 1 On the Utilities menu, click **LiveUpdate**.
- 2 Click **Update Everything Now**.  
A status dialog box keeps you informed of the file transfer process.

## Customize a LiveUpdate session

If you want to update only one or two items, you can select them and omit items that you don't want to update.

### To customize a LiveUpdate session

- 1 In the LiveUpdate window, click **Customize this Update Session**.  
LiveUpdate presents a list of available updates. By default, all are checked for inclusion in this update session. If your files are already up-to-date, no items are available for selection.
- 2 Uncheck the items that you don't want to update.
- 3 Click **Update**.  
The file transfer takes a few minutes. When it is complete, the LiveUpdate summary window appears.

See "View the LiveUpdate Summary" on page 35.

## After updating

When a LiveUpdate session is complete, the LiveUpdate Summary window displays a list of what was updated, along with brief notes.

## View the LiveUpdate Summary

The LiveUpdate Summary dialog box displays a summary of the activity and a list of products updated in this session.

Some updates require that you restart your computer. When this recommendation appears in the summary description, the Restart button is available.

### To restart after a LiveUpdate session

- ❖ In the LiveUpdate Summary window, click **Restart**.

## Empty the Trash after a LiveUpdate session

After you update program files, LiveUpdate moves the older, discarded files to the Trash. If you haven't already restarted after updating, you might get a message that these files are in use. After you restart your computer, you can empty the Trash.

## Check product version numbers and dates

The LiveUpdate window displays the version numbers and dates of the most recent updates.

You can also check the version numbers and dates in the product's About box, accessible from the product menu, to verify that you have the latest version.

### To view an application's About box

- 1 Open your product.
- 2 On the product menu, click **About <product name>**.  
The About box lists the version number and copyright dates.
- 3 When you've finished viewing the About box, close it.

## Schedule future updates



The user who scheduled the event must be logged on for the scheduled event to occur. If this condition is not true, the event occurs the next time the correct user is logged on.

You can set up events to run at a scheduled time, without your participation. If your Macintosh is turned off during the time an event should take place, the event occurs the next time that you start your Macintosh. Before scheduling an update, test it once manually. See [“Update everything now”](#) on page 35, and [“Customize a LiveUpdate session”](#) on page 35.

For instructions on scheduling future updates, see [“Schedule LiveUpdate events”](#) on page 38.

# Scheduling future events

# 5

Use Norton Scheduler to ensure that key tasks are performed regularly to keep your computer and data protected.

## About Norton Scheduler

The tasks that are available in Norton Scheduler depend on what products are installed.

If your Macintosh is turned off during the time that an event should take place, the event occurs the next time that you start your Macintosh.

## Open Norton Scheduler

You can open Norton Scheduler from your open program.

### To open Norton Scheduler from Norton AntiVirus

- 1 Open Norton AntiVirus.
- 2 On the toolbar, click **Norton Scheduler**.

### To open Norton Scheduler from LiveUpdate

- 1 Open LiveUpdate.
- 2 In the LiveUpdate window, click **Norton Scheduler**.

See ["How to start and exit Norton AntiVirus"](#) on page 25.

See ["Update procedures"](#) on page 34.

# Schedule LiveUpdate events

In Norton Scheduler, LiveUpdate events check for updates to your installed products. If you have Norton AntiVirus installed, a monthly *virus definitions* update is also scheduled.

See “Open Norton Scheduler” on page 37.

## To add scheduled LiveUpdate events

- 1
- Open Norton Scheduler.
- 2
- In the Norton Scheduler window, click **New**.
- 3
- Click **Product Update**.
- 4
- Type a descriptive name for the LiveUpdate task, for example, Update Fridays.
- 5
- In the Choose a product to update list, select the item to update. Your options are:

|                   |   |
|-------------------|---|
| All Products      | Updates all installed products.   |
| Virus Definitions | Updates virus definitions.  |
| LiveUpdate        | Updates LiveUpdate program files.   |
| <Product Name>    | Updates a product that you select. The names of installed Symantec products appear in the list. |

- 6
- In the Set a Frequency list, specify when the update should occur. Your options are:

|          |  |
|----------|--|
| Monthly  | Runs the event monthly on the indicated date and time. You can select a date from the first of the month to the twenty-eighth. |
| Weekly   | Updates once a week on the specified day and at the specified time.  |
| Daily    | Runs the event daily at the indicated time.  |
| Annually | Runs the event each year on the indicated day and time. You can schedule the event up to one year in advance.                  |

- 7
- If you choose a frequency other than Daily, specify the date or day of the week that the update should occur.

See "Set a start time" on page 40.

- 8 Set a start time for the event.
- 9 Click **Save**.

## Schedule Norton AntiVirus scans

If you have Norton AntiVirus installed, you can add scheduled scans of all or a part of your computer.

### To add scheduled Norton AntiVirus scans

See "Open Norton Scheduler" on page 37.

- 1 Open Norton Scheduler.
- 2 In the Norton Scheduler window, click **New**.
- 3 Click **AntiVirus Scan**.
- 4 In the Add AntiVirus Scan Task window, type a descriptive name for the task, for example, Scan OS X disk.
- 5 Do one of the following:

■ Drag the item you want to scan from the Finder into the Add AntiVirus Scan Task window.

■ Click **Browse** to select the item you want to scan.
- 6 In the Set a Frequency list, specify when the scan should occur. Your options are:

See "Select an item for a scheduled scan" on page 40.

|          |  |
|----------|--|
| Monthly  | Runs the event monthly on the indicated date and time. You can select a date from the first of the month to the twenty-eighth. |
| Weekly   | Updates once a week on the specified day and at the specified time.  |
| Daily    | Runs the event daily at the indicated time.  |
| Annually | Runs the event each year on the indicated day and time. You can schedule the event up to one year in advance.                  |

See "Set a start time" on page 40.

- 7 If you choose a frequency other than Daily, specify the date or day of the week that the scan should occur.
- 8 Set the time of day that the event should occur.
- 9 Click **Save**.

## Select an item for a scheduled scan

You can select a disk, volume, folder, or file to scan.

### To select an item to scan

- 1 In the Add AntiVirus Scan Task window, click **Browse**.
- 2 In the Select a scan target window, locate the disk, volume, folder, or file.
- 3 Click **Select**.
- 4 The item's name and location appear in the Add AntiVirus Scan Task window.

## Set a start time

You can set the exact time at which you want a scheduled event to start.

### To set a start time

- 1 In the task window, in the Set the time box, do one of the following:
  - Type the exact time that you want in the hour and minute boxes.
  - Select the hour or minute box, then click the Up Arrow or Down Arrow to change the time that is displayed.
- 2 If your computer is set to display a 12-hour clock, an AM/PM indicator appears next to the time. Click the indicator to toggle the setting.
- 3 When you are finished, click **Save**.

## Manage scheduled events

You can edit, delete, disable, and reset scheduled events.

## Edit scheduled events

You can make changes to the events that you schedule.

### To edit a scheduled event

- 1 Open Norton Scheduler.
- 2 In the Scheduled Events list, select the scheduled event that you want to change.
- 3 Click **Edit**.



- 4 Make your changes.  
For a description of the scheduling options, see [“Schedule LiveUpdate events”](#) on page 38.
- 5 To change the event name, type a new name in the name field.
- 6 Click **Save**.

## Delete scheduled events

You can delete scheduled events that you no longer want.

### To delete a scheduled event

- 1 Open Norton Scheduler.
- 2 In the Scheduled Events list, select the scheduled event that you want to delete.
- 3 Click **Delete**.
- 4 In the verification box that appears, click **Delete** to verify that you want to delete the event.

## Disable scheduled events

You can disable scheduled events without deleting them in case you want to enable them later.

### To disable a scheduled event

- 1 In the Scheduled Events list, under On, uncheck the event that you want to disable.
- 2 To enable the event, check it again.

## Reset scheduled tasks

You can reset all scheduled tasks to their original installed settings.

| Product                  | Installed settings   |
|--------------------------|--|
| Norton Personal Firewall | None.  |
| Norton AntiVirus         | Monthly LiveUpdate task to check for new virus definitions. Set to run on the first of each month. |
| Norton Internet Security | Monthly LiveUpdate task to check for new virus definitions. Set to run on the first of each month. |

| Product            | Installed settings   |
|--------------------|--|
| Norton Utilities   | Daily FileSaver snapshot to update your disk directory information. Set to run at noon.<br>Daily Speed Disk defragmentation. Set to run at midnight.   |
| Norton SystemWorks | Monthly LiveUpdate task to check for new virus definitions. Set to run on the first of each month.<br>Daily Speed Disk defragmentation. Set to run at midnight.<br>Daily FileSaver snapshot to update your disk directory information. Set to run at noon. |

To reset scheduled tasks

- 1
- On the Norton Scheduler menu, click **Reset Scheduled Tasks**.
- 2
- In the verification window, click **Reset**.

# Protecting disks, files, and data from viruses

# 6

Although Norton AntiVirus Auto-Protect monitors your computer for viruses by scanning files when they are created or copied, and scanning all disks and removable media when they are mounted, Auto-Protect might not catch new viruses. With Norton AntiVirus you can scan any file, folder, or disk for viruses.

## Scan disks, folders, and files

Start the Norton AntiVirus main program to scan your disks.

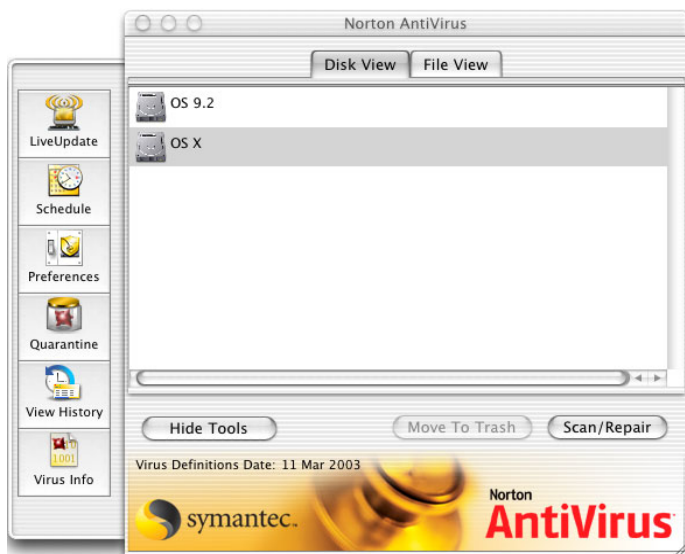
Norton AntiVirus can scan only those files to which you have access permission. Even if you are logged on as an administrator, there are certain system files and directories that cannot be scanned. Those files can be scanned only if you are logged on with root access. However, unless you log on as root when you work on your computer, there is almost no chance that those files could be infected, as Mac OS X is set by default to have the root account disabled. If you never log on as root, performing scans while logged on as an administrator catches any viruses the computer might have acquired.

See ["To check your login type"](#) on page 16.

You can customize the way Norton AntiVirus performs scans. Norton AntiVirus can check *compressed files* for viruses, but not encrypted files. Encrypted files, which normally require a password to open them, must be decrypted before you scan them.

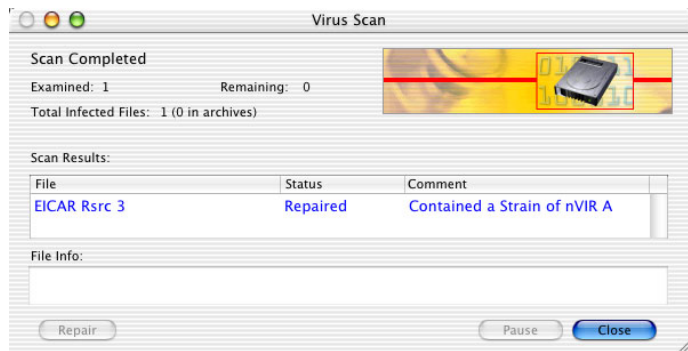
## To scan disks, folders, and files for viruses

- 1 Open Norton AntiVirus.



- 2 In the Norton AntiVirus main window, do one of the following:
  - In Disk View, select the disk to scan.
  - In File View, select individual folders or files to scan.
- 3 Click **Scan/Repair**.
- 4 Click **Pause** to interrupt a scan.  
To resume the scan, click **Continue**.

- 5 To view details of a selected file, look in the Scan Results pane.



- 6 To view details of a selected file, look in the File Info panel.

## If problems are found during a scan

Norton AntiVirus is designed to help keep your computer virus-free. In most cases, an infected file can be repaired automatically. In some cases, you may need to take further action.

In Mac OS X, the file is automatically repaired if you have Automatic Repair On checked on the General tab of the Preferences window.

If the virus is not repaired, the file can be quarantined. Quarantining a file prevents it from reinfecting your computer or damaging other files.

## Scan email attachments

See [“Set Scan Preferences”](#) on page 57.

Norton AntiVirus Auto-Protect provides automatic scanning of email messages. With Auto-Protect enabled and Scan [compressed files](#) turned on, scanning of email is fully functional.

## Scan and repair in archives

The Norton AntiVirus application automatically scans and repairs inside file archives. For example, if you open a zip file Norton AntiVirus scans and, if needed, repairs files without user action.



Scanning of Stuffit file Archives is limited to the Norton AntiVirus application. Auto-Protect, the command line scanner, Scan on Mount, and scheduled scanning do not scan within Stuffit Archives. All other compressed and archival file formats are scanned.

## View and print scan history

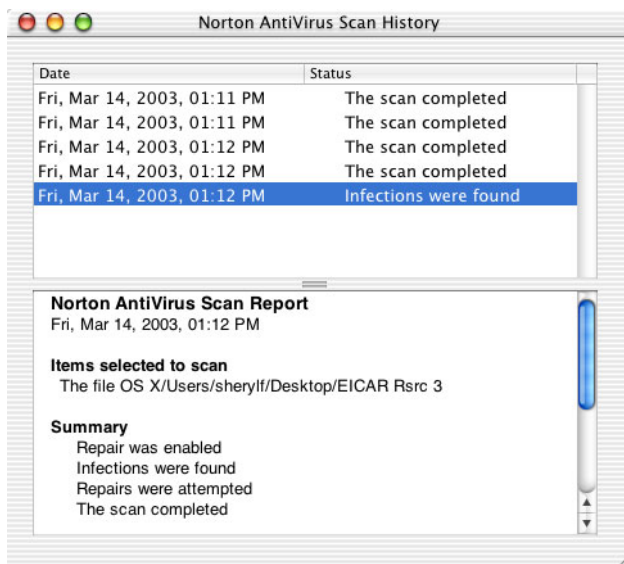
Norton AntiVirus automatically saves a report of each scan. You can view and print these scan results at the end of a scan. You can also review previous scans in the History file.

## Save and print scan reports

At the end of a scan, you can save the scan results in a file. You can specify the file format in Preferences. Saving a scan report in a specific file format associates it to a word processing program. You can print a scan report from the Scan Results window or from the Scan History window.

### To select a scan report to save or print

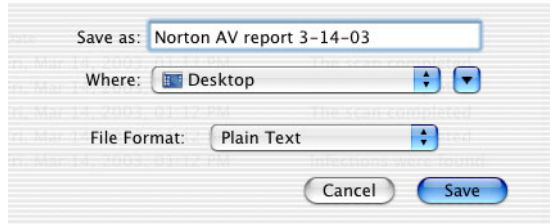
- 1 In the Norton AntiVirus main window, click **View History**.



- 2 In the Norton AntiVirus Scan History window, in the top pane, select the report to view.  
The details appear in the lower pane of the window.

### To save the selected scan report

- 1 On the File menu, click **Save Report As**.
- 2 In the dialog box that appears, specify a name and location for the file. The default file name is <Untitled Report>.



- 3 Click **Save**.

### To print the selected scan report

- 1 Do one of the following:
  - If you are still viewing the scan results, click **Print**.
  - If you have selected the report in the Scan History window, on the File menu, click **Print**.
- 2 In the Print dialog box, select the printing options for the report.
- 3 Click **Print**.

## Perform a scan from the command line

Use the Command Line Scanner to run scans from the command line and to obtain scan reports and save them. Create scripts to be incorporated into other UNIX maintenance scripts.

You can customize the features of the Command Line Scanner to run the scans that you want. Here are a few examples of command line scans you can run:

- `navx /`  
Scans your system drive with default options
- `navx -a -r /Users/steve/`  
Scans without repairing, the files in the home folder of user steve, and report the status of all files

- `navx -ar /Users/steve/`  
Scans without repairing, the files in the home folder of user steve, and reports the status of all files
- `navx -o ~/myReportFile /tmp`  
Scans the files in /tmp, and stores the report in your home folder
- `navx -a -o ~/myReportFile /tmp > <filename.log>`  
Scans the files in /tmp, and stores the complete report in your home folder, and in a log

To scan a file using the Command Line Scanner

- 1 Open Terminal.
- 2 At the prompt, type **navx**.
- 3 Type the command you want. Your options are:

|                      |   |
|----------------------|---|
| -a                   | Reports all files scanned regardless of damage or threat.   |
| -c                   | Scans inside of compressed files.   |
| -f                   | Forces the scan to run even if the output file specified with -o cannot be created or opened.   |
| -h                   | Reports on files that were inaccessible for scanning.   |
| -Q                   | Quarantines files that can't be repaired.   |
| -r                   | Does not repair files with defined threats.   |
| -v                   | Displays the version number.  |
| -o <output filename> | Output appends to the file <output filename>. If -Q is also selected, only the summary appears on the screen, but the full report is appended to <output filename>. |

- 4 Type the name of the file you want to scan.
- 5 Press **Enter**.



# What to do if a virus is found

# 7

If Norton AntiVirus reports a problem follow the instructions provided for that specific problem.

The message may not be discussed in this chapter. For more information about other messages, see [“Troubleshooting in Norton AntiVirus”](#) on page 59.

## Auto-Protect finds a virus

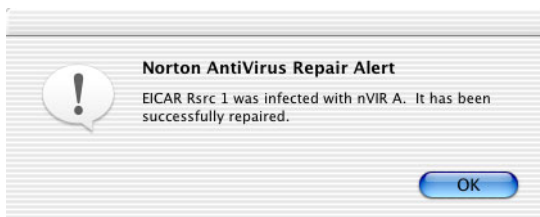
Norton AntiVirus Auto-Protect guards against viruses as soon as your computer starts. It checks programs for viruses as they are run and monitors your computer for any activity that might indicate the presence of a virus. Auto-Protect alerts you to any virus activity.

By default, Auto-Protect is turned on. With default settings, Auto-Protect automatically repairs files or quarantines irreparable files.

When a virus is found while Norton AntiVirus Auto-Protect is running, an [alert](#) displays what happened and what your options are. Read the message carefully to determine whether you need to do anything.

## Auto-Protect finds a virus and repairs the file

When Norton AntiVirus Auto-Protect reports that it repaired an infected file, you don't have to do anything.



Even when Auto-Protect has repaired the infected file, ensure that no other viruses exist on your computer by scanning with Norton AntiVirus.

## Auto-Protect finds a virus but does not repair the file

See ["About User Preferences"](#) on page 56.

If you have set the Auto-Repair Scan preference to Manually repair infected files, Auto-Protect informs you of infected files, but does not repair them.

### To manually repair an infected file that has been detected but not repaired

- 1 Read the entire message.  
Look for words that identify the type of problem.



**2 Click Yes.**

If the file cannot be repaired it is automatically quarantined. For more information about quarantine settings, see [“About User Preferences”](#) on page 56.



**3 Click OK.**

## Auto-Protect finds a virus and cannot repair the file

In a few cases, Auto-Protect may not be able to repair or quarantine an infected file, whether or not you have preferences set to Automatic Repair.

### To delete an infected file that has been detected but cannot be repaired

See [“Scan disks, folders, and files”](#) on page 43.

- ❖ Click **Yes** to run Norton AntiVirus and scan the file or folder containing the virus.  
 In the scan window, you can view more details about the infected file.  
 See [“If Norton AntiVirus can’t repair a file”](#) on page 53.

## A virus is found when removable media is inserted

If Auto-Protect finds a virus when [removable media](#) is connected to your computer, an [alert](#) displays what happened and what your options are. See [“Auto-Protect finds a virus”](#) on page 49 and [“A virus is found during a user-initiated scan”](#) on page 52.

## Repair, Delete, and Restore in Quarantine

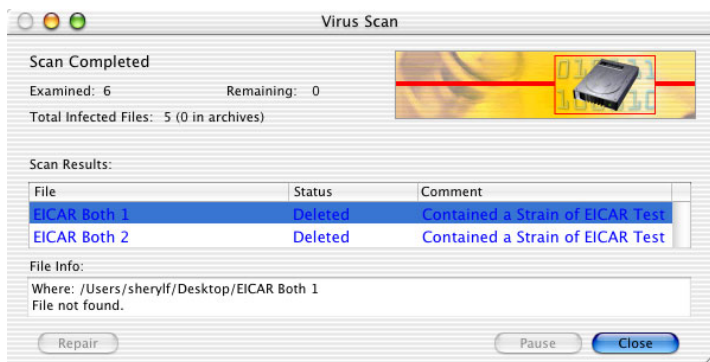
After files have been quarantined you can try to repair, delete, or restore the file.

## A virus is found during a user-initiated scan

If you are scanning with Norton AntiVirus and a virus is found, a Problem found *alert* appears in the scan window. Usually, infected files are repaired or quarantined automatically and you don't have to do anything else. To determine if the file was repaired or if you need to take further action, check the status of the file in the scan window.

### To check the status of infected files in the scan window

- ❖ In the Virus Scan window, under Scan Results, select the infected file.



## Repair infected files

If an infected file in the scan window was not repaired because Auto-Repair was turned off in Preferences and you have Quarantine files that cannot be repaired unchecked, initiate the repair yourself.

### To repair infected files

- 1 In the scan results list, select the files to repair.
- 2 Click **Repair**.
- 3 After repairing all infected files, scan your disks again to verify that there are no other infected files.
- 4 Check the repaired files to make sure that they function properly. For example, if you repaired a word processing program, start it, edit a file, save a file, and so on to make sure that it has been repaired correctly.

## If Norton AntiVirus can't repair a file

See ["Check product version numbers and dates"](#) on page 36.

If Norton AntiVirus cannot repair the infected file, first make sure you have scanned with the latest [virus definitions](#). If you are not sure that you have the latest definitions, use LiveUpdate. Then scan your hard disk with the latest virus definitions.

## If removable media is infected

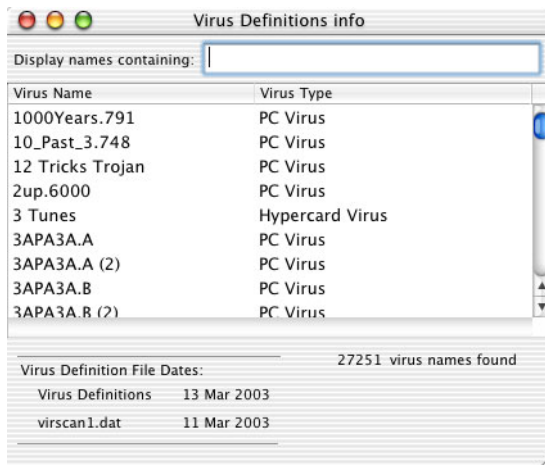
To repair the infected media, use Norton AntiVirus to scan and repair it.

### To repair infected removable media

- 1 Open Norton AntiVirus.
- 2 In the Norton AntiVirus main window, select the media to scan.
- 3 Click **Scan/Repair**.

## Look up virus names and definitions

You can look up a virus name from within the Norton AntiVirus application. The Virus Definitions Info dialog box lists the viruses in the current [virus definitions](#) file. To make sure you have the latest virus definitions, run LiveUpdate. You can export the list to a text file. You can also search the list for a specific virus.



**Look up virus names and definitions****To look up virus names**

- 1 On the Tools menu, click **Virus Info**.
- 2 Type the name or part of the name of the virus.

## Look up virus definitions on the Symantec Web site

Because of the large number of viruses, the Virus Definitions Info file does not include descriptions of each virus. The Symantec Security Response Web site contains a complete list of all known viruses and related malicious code, along with descriptions.

**To look up virus definitions**

- 1 Point your browser to the Symantec Security Response Web site at: <http://securityresponse.symantec.com>
- 2 Click **Expanded Threat List and Virus Encyclopedia**.
- 3 Do one of the following:
  - Type a virus name for which to search.
  - Scroll through the alphabetical list to locate a virus.
- 4 Click a virus to read its description.

Norton AntiVirus provides the best virus detection and removal with default settings left on. If you want to change the default settings because you want to extract data from a file before it is deleted or repaired due to a virus, you can.

There are three types of preferences to set. Your options are:

|                 |   |
|-----------------|---|
| Scan and Repair | Settings that govern the behavior of the Norton AntiVirus application and settings separate users can specify |
| Auto-Protect    | Settings that govern the behavior of overall antivirus protection and repair for your computer                |
| Reminder        | Settings for the Virus Definition Alert preference  |

## About Auto-Protect Preferences

Active Auto-Protect settings provide you with continuous and ceaseless antivirus protection. You can however change automatic antivirus protection settings if you want to manually repair or delete a file or if you want to manually scan *removable media* when it is inserted.

You can change a range of settings for the way Norton AntiVirus Auto-Protect repairs files.




For maximum protection leave Auto-Protect on and do not change default preferences in the Norton Auto-Protect window.

## Set Auto-Protect Preferences

Determine how you want Norton Auto-Protect to monitor viruses and repair infected files.

### To set Auto-Protect Preferences

- 1 In the Norton AntiVirus main window, click **Preferences**.
- 2 In the Preferences window, click the **Auto-Protect** tab.
- 3 Click **Launch Auto-Protect Preferences**.
- 4 In the Norton Auto-Protect window, click the lock icon to make changes.
- 5 In the Authenticate dialog box, type your administrator name and password.
- 6 Click **OK**.
- 7 Select the Auto-Protect options that you want. Your options are:

|                         |   |
|-------------------------|---|
| Auto-Protect            | Provides automatic virus monitoring.<br> If you turn Auto-Protect off all other automatic options are unavailable. |
| Automatic Repair        | Automatically repairs infected files found.   |
| Quarantine              | Automatically quarantines files that cannot be repaired.  |
| Scan Disks when mounted | Automatically scans removable media such as CDs, Zip drives, or an iPod when they are inserted in your computer.  |
| Scan compressed files   | Automatically scans compressed files.   |

- 8 Close the window to save your changes.

## About User Preferences

You can change the preferences that were set up when you installed Norton AntiVirus for Macintosh. Moreover, individual users can specify their Norton AntiVirus settings.



For maximum protection do not change default preferences in the Scan, Repair, and Reminder tabs.



# Set Scan Preferences

Determine how you want Norton AntiVirus to scan disks and files.

## To set Scan Preferences

- 1
- In the Norton AntiVirus main window, click **Preferences**.
- 2
- In the Preferences window, on the Scan tab, select the options that you want. Your options are:

|                       |  |
|-----------------------|--|
| Scan compressed files | Scan compressed files. Scanning time will be longer if you scan compressed files.  |
| Scan Results          | Determine which files you want listed in the Scan Results pane of the Scan window. |
| Scheduled Scan Alerts | Specify if you want a scan alert always or only when infected files are found.     |
| Report Format         | Select the program in which to view saved antivirus reports.                       |

- 3
- Click **Save**.

# Set Repair Preferences

Determine how you want Norton AntiVirus to repair infected files found during a manual scan.

## To set Repair Preferences

- 1
- In the Norton AntiVirus main window, click **Preferences**.
- 2
- In the Preferences window, click the **Repair** tab.
- 3
- Select the Repair options that you want. Your options are:

|  |   |
|--|---|
| Repair                                   | During a manual scan, set to repair infected files found automatically or manually.     |
| Quarantine files that cannot be repaired | During a manual scan, select to automatically quarantine files that cannot be repaired. |

- 4
- Click **Save**.

## Set a Reminder

You can set Norton AntiVirus to notify you when your *virus definitions* are out-of-date. The latest virus definitions are necessary to keep your computer virus-free.

## Customize the Norton QuickMenu

The Norton QuickMenu appears as the yellow-and-black Symantec logo on the right side of the menu bar on the top of your screen. If you do not want the Norton QuickMenu to appear on your menu bar, you can hide it. You can also change the items that appear on the menu.

### To hide the Norton QuickMenu

- 1 On the Norton QuickMenu, click **Norton QuickMenu > Preferences**.
- 2 In the Norton QuickMenu window, uncheck **Enable Norton QuickMenu**.
- 3 On the System Preferences menu, click **Quit System Preferences**.

### To show the Norton QuickMenu

- 1 On the Apple menu, click **System Preferences**.
- 2 In the System Preferences window, click **Norton QuickMenu**.
- 3 In the Norton QuickMenu window, check **Enable Norton QuickMenu**.
- 4 On the System Preferences menu, click **Quit System Preferences**.

### To change what appears on the Norton QuickMenu

- 1 On the Norton QuickMenu, click **Norton QuickMenu > Preferences**.
- 2 In the Norton QuickMenu window, uncheck the items that you do not want to appear on the menu.
- 3 On the System Preferences menu, click **Quit System Preferences**.

# Troubleshooting in Norton AntiVirus

# 9

The problems discussed are not directly related to virus activity. If you cannot resolve your problem, consult the Read Me file on the Norton AntiVirus for Macintosh CD.

For a comprehensive list of the latest troubleshooting tips, see the Symantec Service and Support Web site at:  
[www.symantec.com/techsupp/](http://www.symantec.com/techsupp/)

## Installation problems

See ["Installing Norton AntiVirus"](#) on page 15.

If you encounter any problems installing Norton AntiVirus, try restarting and installing Norton AntiVirus again. Or, make a copy of the Mac OS X installer from the Norton AntiVirus for Macintosh CD and paste it onto your computer and install from there.

## I can't install Norton AntiVirus

You must start your computer in Mac OS X to run the Norton AntiVirus for Mac OS X installer. And you must know your administrator password to install Norton AntiVirus.

## Startup problems

Startup problems could be due to problems with your computer, with Norton AntiVirus, or with settings that you have made.

## Norton AntiVirus Auto-Protect fails to load when I start my Macintosh

If Auto-Protect fails to load, make sure that all engine files and virus definitions are installed. Norton AntiVirus Auto-Protect does not run without them.

## Norton AntiVirus reports that a file is invalid when trying to launch or scan, or at startup

This is an indication that one of the files making up the *virus definitions* is damaged or otherwise invalid.

### To repair a damaged virus definitions file in Mac OS X

- 1 Uninstall Norton AntiVirus.
- 2 Reinstall Norton AntiVirus.
- 3 Run LiveUpdate and update your virus definitions.  
This restores the current versions of the items in the Norton AntiVirus Additions folder.

See ["Installation"](#) on page 16.

## Norton AntiVirus cannot find the Norton AntiVirus virus definitions file

Reinstall Norton AntiVirus.

## Why can't I create an alias to Norton AntiVirus?

If you did not install Norton AntiVirus, you cannot create an alias to it because of the access permissions established in Mac OS X. Have the person who installed the software create an alias and place the alias in an area to which you have access. You can then drag the alias to the location that you want.

# Protection problems

A file on the disk may be damaged, or Norton AntiVirus ran out of memory, or some other error occurred during scanning.

## To determine if a file is causing the problem

See "How to start and exit Norton AntiVirus" on page 25.

- 1 Open Norton AntiVirus.
- 2 On the File View tab, click the drive triangle to display the folders inside.
- 3 Scan the folders one at a time to determine where the problem is occurring.
- 4 Scan your disk again from the Norton AntiVirus main window. You may also want to examine the disk using a program such as Norton Disk Doctor (part of Norton Utilities for Macintosh).

## Scanning and account access privileges

Norton AntiVirus scans only those files for which your account has access privileges. If you ever log on and work as root, run the scan while logged on as root. If you do not log on as root, running the scan while logged on as an Administrator scans all files that could be infected while using that logon. If you do not want to see the list of files that could not be scanned because of denied access, check Do not list permissions errors when scanning in Preferences.

## I need to rescan files that have already been scanned

The Norton AntiVirus QuickScan file records whether you have already scanned a file using the currently installed virus definitions and libraries. If not, the file is scanned. If you want all files to be scanned regardless, you can use Norton AntiVirus to delete the QuickScan file at the root of each disk. The file is named NAVMac800QSFFile.

## To remove the QuickScan file

- 1 In the Norton AntiVirus window, on the File View tab, ensure that Show Invisible Files is checked.
- 2 Select your hard disk.
- 3 Click the **QuickScan** file.  
If there are QuickScan files from previous versions of Norton AntiVirus, select them as well.
- 4 Click **Move To Trash**.

- 5 Click **OK**.
- 6 Quit Norton AntiVirus.
- 7 In the Finder, click **Empty Trash**.

After you have deleted the QuickScan file, the first scan with the new *virus definitions* will be slower.

## I'm having trouble updating virus definitions using LiveUpdate

In some rare cases such as immediately after the emergence of a new virus, the LiveUpdate servers may be very busy and it may be difficult to get a connection. In such cases, keep making connection attempts and you should eventually be successful.

When using LiveUpdate, make sure that your Internet connection is working by testing the connection with an application, such as your Web browser.

## Other troubleshooting steps

Here are some other steps that you can take to resolve problems with your Macintosh:

- Reinstall or upgrade the System software.  
For more information, see your Macintosh System documentation.
- Reinstall Norton AntiVirus.
- Reset the PRAM (Parameter RAM).  
For more information, see your Macintosh System documentation.

See "Installing  
Norton AntiVirus"  
on page 15.

## Error messages

The following messages might be encountered when you are running Norton AntiVirus and Norton AntiVirus Auto-Protect.

Norton AntiVirus uses available memory to store items for the scan report. If you have many files, you will not be able to record all items to scan. You can change the Report Preferences to record infected files only.

## Auto-Protect error message

If you experience problems with the scan engine error message, you might still have incompatible files from a previous version of Norton AntiVirus for Macintosh. Uninstall and then reinstall Norton AntiVirus.

## Password and administrator messages

**The entered subscription code is not valid. Please retype in the 9 character subscription code again.**

You entered a virus definitions subscription code incorrectly. Try typing the number again.

**The passwords did not match. Please try again.**

The second password you typed does not match the first one.

**That password is incorrect. Please try again.**

You typed an incorrect password. If you forgot your password, see [“Installation”](#) on page 16.

**The software to be installed requires Administrator or higher level access privileges.**

Enter your administrator password.





# Using Norton AntiVirus on a network



You can run Norton AntiVirus on any AppleTalk Transaction Protocol server such as AppleShare or TOPS.

## Notes to the administrator

Set up Norton AntiVirus the following way in a networking environment:

- Run Norton AntiVirus Auto-Protect and the Norton AntiVirus application on the system administrator's computer.
- Make sure Norton AntiVirus Auto-Protect is run on all workstation Macintosh computers.
- Use the Scheduler command from the Norton AntiVirus Tools menu to schedule periodic scans of all network drives.

## Scanning network drives

When you are scanning network drives from a workstation, the server slows down for other users. If others are creating, deleting, or moving files on a network drive while Norton AntiVirus is scanning, all files may not get scanned.

To prevent files from not getting scanned, do the following:

- Make sure that you are the only one logged on to the server when scanning network drives.
- Shut down the server, restart, reinstall Norton AntiVirus, and then perform the scan.

## Preparing an emergency response plan

To be fully prepared in case of a virus attack on a workstation, be sure to have a detailed emergency response plan written and distributed within your networking group before a problem arises. This maintains order and prevents panic in case of an infection.

Complete your plan based on the dynamics and needs of your organization.

### Before a virus is detected

Conduct an informational meeting with your network users to discuss the basic nature and behavior of computer viruses. Stress that while having a computer virus on your system is reason to take immediate action, there is no need to panic. Emphasize that many viruses spread from illegal software copies, and prohibit the use of such software in your organization. Finally, explain how you've configured Norton AntiVirus to respond to a virus.

Instruct your users to:

- Scan all software before using it. This includes programs downloaded from the Internet as well as new software.
- Watch for warning signs such as frequent system crashes, lost data, screen interference, or suddenly unreliable programs.
- Keep a current store of virus-free program backups.
- Avoid running programs from unscanned removable media.
- Write-protect removable media before using it in someone else's computer.

To protect the workstations:

- Scan each workstation to make sure that it is virus-free.
- Train your users to use a file backup utility on a regular basis.
- Train your users to update the virus definitions file when it becomes available.

To protect the network:

- Password-protect all network executable directories so that only the administrator has write access to them.
- Scan for viruses on new and rented computers before using them.
- Schedule periodic scans of all network servers.
- If you are using Novell NetWare or Windows NT servers, use Norton AntiVirus Enterprise Solution components to protect servers from virus infections.

## **If a virus is detected**

If a virus is detected on your network, remove it from all computers attached to the network.

### **To remove a virus**

- 1** Physically disconnect the workstation from the network.
- 2** Eradicate the virus on the workstation before reconnecting to the network.
- 3** Notify other users on the network to scan for viruses immediately.
- 4** Scan your network servers for viruses.



# Service and support solutions

The Service & Support Web site at <http://service.symantec.com> supports Symantec products. Customer Service helps with nontechnical issues such as orders, upgrades, replacements, and rebates. Technical Support helps with technical issues such as installing, configuring, or troubleshooting Symantec products.

Methods of technical support and customer service can vary by region. For information on support offerings in your region, check the appropriate Web site listed in the sections that follow.

If you received this product when you purchased your computer, your computer manufacturer may be responsible for providing your support.

## Customer service

The Service & Support Web site at <http://service.symantec.com> tells you how to:

- Subscribe to Symantec newsletters.
- Locate resellers and consultants in your area.
- Replace defective CD-ROMs and manuals.
- Update your product registration.
- Find out about orders, returns, or a rebate status.
- Access Customer Service FAQs.
- Post a question to a Customer Service representative.
- Obtain product information, literature, or trialware.

For upgrade orders, visit the Symantec Store at:  
<http://www.symantecstore.com>

## Technical support

Symantec offers two technical support options for help with installing, configuring, or troubleshooting Symantec products:

- **Online Service and Support**  
Connect to the Symantec Service & Support Web site at <http://service.symantec.com>, select your user type, and then select your product and version. You can access hot topics, Knowledge Base articles, tutorials, contact options, and more. You can also post a question to an online Technical Support representative.
- **PriorityCare telephone support**  
This fee-based (in most areas) telephone support is available to all registered customers. Find the phone number for your product at the Service & Support Web site. You'll be led through the online options first, and then to the telephone contact options.

## Support for old and discontinued versions

When Symantec announces that a product will no longer be marketed or sold, telephone support is discontinued 60 days later. Technical information may still be available through the Service & Support Web site at:  
<http://service.symantec.com>

## Subscription policy

If your Symantec product includes virus, firewall, or Web content protection, you may be entitled to receive updates via LiveUpdate. Subscription length varies by Symantec product.

After your initial subscription ends, you must renew it before you can update your virus, firewall, or Web content protection. Without these updates, you will be vulnerable to attacks.

When you run LiveUpdate near the end of your subscription period, you are prompted to subscribe for a nominal charge. Simply follow the instructions on the screen.

## Worldwide service and support

Technical support and customer service solutions vary by country. For Symantec and International Partner locations outside of the United States, contact one of the service and support offices listed below, or connect to <http://service.symantec.com> and select your region under Global Service and Support.

## Service and support offices

### **North America**

Symantec Corporation  
555 International Way  
Springfield, OR 97477  
U.S.A.

<http://www.symantec.com/>

### **Australia and New Zealand**

Symantec Australia  
Level 2, 1 Julius Avenue  
North Ryde, NSW 2113  
Sydney  
Australia

[http://www.symantec.com/region/reg\\_ap/](http://www.symantec.com/region/reg_ap/)  
+61 (2) 8879-1000  
Fax: +61 (2) 8879-1001

### **Europe, Middle East, and Africa**

Symantec Customer Service Center  
P.O. Box 5689  
Dublin 15  
Ireland

[http://www.symantec.com/region/reg\\_eu/](http://www.symantec.com/region/reg_eu/)  
+353 (1) 811 8032

### **Latin America**

Symantec Brasil  
Market Place Tower  
Av. Dr. Chucri Zaidan, 920  
12 andar  
São Paulo - SP  
CEP: 04583-904  
Brasil, SA

Portuguese:  
<http://www.service.symantec.com/br>  
Spanish:  
<http://www.service.symantec.com/mx>  
Brazil: +55 (11) 5189-6300  
Mexico: +52 55 5322 3681 (Mexico DF)  
01 800 711 8443 (Interior)  
Argentina: +54 (11) 5382-3802

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

November 25, 2002





# Glossary

|                          |  |
|--------------------------|--|
| <b>access privileges</b> | The types of operations that a user can perform on a system resource. For example, a user can have the ability to access a certain directory and open, modify, or delete its contents. |
| <b>ActiveSync</b>        | The synchronization software for Microsoft Windows-based Pocket PCs.   |
| <b>ActiveX</b>           | A method of embedding interactive programs into Web pages. The programs, which are called controls, run when you view the page.  |
| <b>alert</b>             | A message that appears to signal that an error has occurred or that there is a task that requires immediate attention, such as a system crash or a Virus Alert.                        |
| <b>alias</b>             | A shortcut icon that points to an original object such as a file, folder, or disk.   |
| <b>AppleTalk</b>         | A protocol that is used by some network devices such as printers and servers to communicate.   |
| <b>attack signature</b>  | A data pattern that is characteristic of an Internet attack. Intrusion Detection uses attack signatures to distinguish attacks from legitimate traffic.                                |
| <b>beam</b>              | To transfer certain programs and data between two handheld devices using built-in infrared technology.   |

|   |   |
|---|---|
| <b>boot record</b>                                | A sector at the start of a disk that describes the disk (sector size, cluster size, and so on). On startup disks, the boot record also has a program that loads the operating system.                       |
| <b>bootable disk</b>                              | A disk that can be used to start a computer.  |
| <b>cache</b>                                      | A location on your disk in which data is stored for reuse. A Web browser cache stores Web pages and files (such as graphics) as you view them.  |
| <b>cache file</b>                                 | A file that is used to improve the performance of Windows.  |
| <b>compressed file</b>                            | A file whose content has been made smaller so that the resulting data occupies less physical space on the disk.   |
| <b>connection-based protocol</b>                  | A protocol that requires a connection before information packets are transmitted.   |
| <b>connectionless protocol</b>                    | A protocol that sends a transmission to a destination address on a network without establishing a connection.   |
| <b>cookie</b>                                     | A file that some Web servers put on your disk when you view pages from those servers. Cookies store preferences, create online shopping carts, and identify repeat visitors.                                |
| <b>denial-of-service attack</b>                   | A user or program that takes up all of the system resources by launching a multitude of requests, leaving no resources, and thereby denying service to other users.   |
| <b>DHCP (Dynamic Host Configuration Protocol)</b> | A TCP/IP protocol that assigns a temporary IP address to each device on a network. DSL and cable routers use DHCP to allow multiple computers to share a single Internet connection.                        |
| <b>dial-up</b>                                    | A connection in which a computer calls a server and operates as a local workstation on the network.   |
| <b>DNS (Domain Name System)</b>                   | The naming system used on the Internet. DNS translates domain names (such as <a href="http://www.symantec.com">www.symantec.com</a> ) into IP addresses that computers understand (such as 206.204.212.71). |

|   |   |
|---|---|
| <b>DNS server (Domain Name System server)</b> | A computer that maps domain names to IP addresses. When you visit <a href="http://www.symantec.com">www.symantec.com</a> , your computer contacts a DNS server that translates the domain name into an IP address (206.204.212.71). |
| <b>domain</b>                                 | The common Internet address for a single company or organization (such as <a href="http://symantec.com">symantec.com</a> ). See also host name.   |
| <b>DOS window</b>                             | A method of accessing the MS-DOS operating system to execute DOS programs through the Windows graphical environment.  |
| <b>download</b>                               | To transfer a copy of a file or program from the Internet, a server, or computer system to another server or computer.  |
| <b>driver</b>                                 | Software instructions for interpreting commands for transfer to and from peripheral devices and a computer.   |
| <b>encryption</b>                             | Encoding data in such a way that only a person with the correct password or cryptographic key can read it. This prevents unauthorized users from viewing or tampering with the data.  |
| <b>Ethernet</b>                               | A common method of networking computers in a LAN (local area network). Ethernet cables, which look like oversized phone cables, carry data at 10M bps or 100M bps.  |
| <b>executable file</b>                        | A file containing program code that can be run. Generally includes any file that is a program, extension, or system files whose names end with .bat, .exe, or .com.   |
| <b>extension</b>                              | The three-letter ending on a file name that associates the file with an activity or program. Examples include .txt (text) and .exe (executable program).  |
| <b>FAT (file allocation table)</b>            | A system table (used primarily by DOS and Windows 9x/Me) that organizes the exact location of the all files on the hard drive.  |
| <b>file type</b>                              | A code that associates the file with a program or activity, often appearing as the file name extension, such as .txt or .jpeg.  |

|  |   |
|--|---|
| <b>Finder</b>                                    | The program that manages your Macintosh disk and file activity and display.   |
| <b>firewall rule</b>                             | Parameters that define how a firewall reacts to specific data or network communications. A firewall rule usually contains a data pattern and an action to take if the pattern is found.                                 |
| <b>fragmented</b>                                | When the data that makes up a file is stored in noncontiguous clusters across a disk. A fragmented file takes longer to read from the disk than an unfragmented file.   |
| <b>fragmented IP packet</b>                      | An IP packet that has been split into parts. Packets are fragmented if they exceed a network's maximum packet size, but malicious users also fragment them to hide Internet attacks.                                    |
| <b>FTP (File Transfer Protocol)</b>              | An application protocol used for transferring files between computers over TCP/IP networks such as the Internet.  |
| <b>hidden attribute</b>                          | A file attribute that makes files harder to access and more difficult to delete than other files. It also prevents them from appearing in a DOS or Windows directory list.  |
| <b>host name</b>                                 | The name by which most users refer to a Web site. For example, <a href="http://www.symantec.com">www.symantec.com</a> is the host name for the Symantec Web site. Host names are translated to IP addresses by the DNS. |
| <b>HotSync</b>                                   | The synchronization software for Palm OS handheld devices.  |
| <b>HTML (Hypertext Markup Language)</b>          | The language used to create Web pages.  |
| <b>ICMP (Internet Control Message Protocol)</b>  | An extension to the basic Internet Protocol (IP) that provides feedback about network problems.   |
| <b>IGMP (Internet Group Management Protocol)</b> | An extension to the basic Internet Protocol (IP) that is used to broadcast multimedia over the Internet.  |

|  |  |
|--|--|
| <b>IMAP<sub>4</sub> (Internet Message Access Protocol version 4)</b> | One of the two most popular protocols for receiving email. IMAP makes messages available to read and manage without downloading them to your computer.                                 |
| <b>infrared (IR) port</b>  | A communication port on a handheld device for interfacing with an infrared-capable device. Infrared ports do not use cables.   |
| <b>IP (Internet Protocol)</b>  | The protocol that underlies most Internet traffic. IP determines how data flows from one computer to another. Computers on the Internet have IP addresses that uniquely identify them. |
| <b>IP address (Internet Protocol address)</b>                        | A numeric identifier that uniquely identifies a computer on the Internet. IP addresses are usually shown as four groups of numbers separated by periods. For example, 206.204.52.71.   |
| <b>ISP (Internet service provider)</b>                               | A company that supplies Internet access to individuals and companies. Most ISPs offer additional Internet connectivity services, such as Web site hosting.                             |
| <b>Java</b>  | A programming language used to create small programs called applets. Java applets can be used to create interactive content on Web pages.  |
| <b>JavaScript</b>  | A scripting language used to enhance Web pages. Most sites use JavaScript to add simple interactivity to pages, but some use it to open pop-up ads and reset visitors' homepages.      |
| <b>macro</b>   | A simple software program that can be started by a specific keystroke or a series of keystrokes. Macros can be used to automate repetitive tasks.                                      |
| <b>NAT (network address translation)</b>                             | A method of mapping private IP addresses to a single public IP address. NAT allows multiple computers to share a single public IP address. Most DSL and cable routers support NAT.     |
| <b>network address</b>   | The portion of an IP address that is shared by all computers on a network or subnet. For example, 10.0.1.1 and 10.0.1.8 are part of the network address 10.0.1.0.                      |

|  |   |
|--|---|
| <b>NTFS (NTFS file system)</b>               | A system table (used primarily by Windows 2000/XP) that organizes the exact location of all the files on the hard drive.  |
| <b>packet</b>                                | The basic unit of data on the Internet. Along with the data, each packet includes a header that describes the packet's destination and how the data should be processed.                  |
| <b>partition</b>                             | A portion of a disk that is prepared and set aside by a special disk utility to function as a separate disk.  |
| <b>POP3 (Post Office Protocol version 3)</b> | One of the two most popular protocols for receiving email. POP3 requires that you download messages to read them.   |
| <b>port</b>                                  | A connection between two computers. TCP/IP and UDP use ports to indicate the type of server program that should handle a connection. Each port is identified by a number.                 |
| <b>port number</b>                           | A number used to identify a particular Internet service. Internet packets include the port number to help recipient computers decide which program should handle the data.                |
| <b>PPP (Point-to-Point Protocol)</b>         | A protocol for communication between two computers using a dial-up connection. PPP provides error-checking features.  |
| <b>protocol</b>                              | A set of rules governing the communication and transfer of data between computers. Examples of protocols include HTTP and FTP.  |
| <b>proxy</b>                                 | A computer or program that redirects incoming and outgoing traffic between computers or networks. Proxies are often used to protect computers and networks from outside threats.          |
| <b>registry</b>                              | A category of data stored in the Windows registry that describes user preferences, hardware settings, and other configuration information. Registry data is accessed using registry keys. |
| <b>removable media</b>                       | Disks that can be removed, as opposed to those that cannot. Some examples of removable media are floppy disks, CDs, DVDs, and Zip disks.  |

|  |   |
|--|---|
| <b>router</b>  | A device that forwards information between computers and networks. Routers are used to manage the paths that data takes over a network. Many cable and DSL modems include routers.        |
| <b>script</b>  | A program, written in a scripting language such as VBScript or JavaScript, that consists of a set of instructions that can run without user interaction.                                  |
| <b>service</b>   | General term for the process of offering information access to other computers. Common services include Web service and FTP service. Computers offering services are called servers.      |
| <b>SSL (Secure Sockets Layer)</b>                                | A protocol for secure online communication. Messages sent using SSL are encrypted to prevent unauthorized viewing. SSL is often used to protect financial information.                    |
| <b>subnet</b>  | A local area network that is part of a larger intranet or the Internet.   |
| <b>subnet mask</b>   | A code, in the form of an IP address, that computers use to determine which part of an IP address identifies the subnet and which part identifies an individual computer on that subnet.  |
| <b>synchronize</b>   | The process by which a handheld device and computer compare files to ensure that they contain the same data.  |
| <b>sync</b>  | The process of transferring programs and data from a computer to a handheld device.   |
| <b>TCP/IP (Transmission Control Protocol/ Internet Protocol)</b> | Standard protocols used for most Internet communication. TCP establishes connections between computers and verifies that data is properly received. IP determines how the data is routed. |
| <b>threat</b>  | A program with the potential to cause damage to a computer by destruction, disclosure, modification of data, or denial of service.  |
| <b>Trojan horse</b>  | A program containing malicious code that is disguised as or hiding in something benign, such as a game or utility.  |

|                                     |  |
|-------------------------------------|--|
| <b>UDP (User Datagram Protocol)</b> | A protocol commonly used for streaming media. Unlike TCP, UDP does not establish a connection before sending data and it does not verify that the data is properly received.   |
| <b>virus definition</b>             | Virus information that an antivirus program uses to identify and alert you to the presence of a specific virus.  |
| <b>wildcard characters</b>          | Special characters (like *, \$, and ?) that act as placeholders for one or more characters. Wildcards let you match several items with a single specification.   |
| <b>worm</b>                         | A program that replicates without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory to slow a computer down. So far, worms do not exist in the Macintosh world. |



# Index

## A

- administrator
  - network 65
  - password 16
- alerts 49-51
- America Online
  - connecting before LiveUpdate 33
  - connecting to Symantec Web site 22
- antivirus newsletter 29
- antivirus scans
  - avoid viruses 13
  - scheduling 39
- AppleTalk 65
- Auto-Protect
  - activation 20
  - description 26, 49
  - finds and repairs virus 50
  - preferences 55-56
  - turning off 27

## B

- Bloodhound 12

## C

- CD-ROM drive, installation alternatives 16
- checking for viruses 43
- Command Line Scanner 48
- command line, scanning from 47

- customizing

- LiveUpdate 35
  - Norton AntiVirus 55-58

## D

- decontamination procedures 46
- deleting, infected file 53
- document, infected 10
- Documentation folder 23

## E

- emergency response plan 66-67

## F

- file
  - repairing infected 52
  - System 10
- files, updating with LiveUpdate 35
- firewalls, using LiveUpdate 33

## G

- getting started 25
- glossary terms 28

## H

- Help
  - accessing 27
  - tips for using 28

**I**

infected file, repairing 52  
installing 15  
instructions, user 66

**K**

keeping files current 31  
Knowledge Base 29

**L**

Late Breaking News 22  
LiveUpdate  
    checking file dates 36  
    customizing 35  
    emptying Trash 36  
    keeping current with 31  
    scheduled events 38  
    updating files 35  
    using with America Online 33  
    viewing summary 35

**M**

macro viruses 10  
messages  
    Auto-Protect 50  
    Norton AntiVirus 63  
Microsoft Excel 10  
Microsoft Office viruses 10  
Microsoft Word 10

**N**

NAV 7.0 QuickScan 61  
network  
    administrator notes 65  
    implementation 65-67  
    protecting 67  
networks, using LiveUpdate 33  
Norton AntiVirus  
    Auto-Protect preferences 55  
    customizing 55  
    description 9  
    messages 63  
    network implementation 65-67

Norton AntiVirus (*continued*)  
    protection after installation 20  
    scheduled events 39  
    updating virus definitions 33

Norton Scheduler  
    changing events 40  
    deleting events 41  
    described 37  
    resetting events 41

**P**

Parameter RAM. *See* PRAM  
PDF 27  
    reading 28  
    tips for using 28  
PRAM 62  
preferences  
    Auto-Protect 56  
    reminder 55  
    user 57  
printing scan report 46-47  
program files, updating with LiveUpdate 35  
protection  
    description 32  
    network 67  
    workstation 66

**R**

Read Me file 16, 23, 28  
    opening on the CD 16  
    password 59  
    troubleshooting 59  
registering your product 20  
repairing infected file 52  
reports  
    administrator 63  
    saving 47  
    viewing scan history 46  
responding to virus alerts 49-53  
restarting, after installation 19

**S**

saving scan report 46  
scan disks when mounted 56

- scan history, saving 46
- scan report
  - printing 47
  - saving 46
- scanning
  - disks 43-45
  - files 43-45
  - folders 43-45
  - history, viewing 46
  - network drives 65
  - with new virus definitions 61
- scheduled events
  - changing 40
  - deleting 41
  - LiveUpdate 38
  - Norton AntiVirus scans 39
  - resetting 41
- Service and Support 69
- service and support Web site 29
- settings
  - LiveUpdate 35
  - preferences 55
- starting, Norton AntiVirus 26
- subscriptions 32
- Symantec AntiVirus for Macintosh
  - deleted during installation 15
  - incompatible with Norton AntiVirus virus definitions 15
- Symantec Security Response
  - newsletter 29
  - Web site 54
- Symantec Web site 29
  - downloading product updates 33
  - tips for searching 29
- system
  - files 10
  - requirements, in Read Me file 16
  - viruses 10

## T

- Technical Support 69
- TOPS 65
- Trash, empty after LiveUpdate session 36
- Trojan horses 10
- troubleshooting 59

## U

- updating
  - all files 35
  - from Symantec Web site 33
- user instructions 66
- User's Guide
  - described 27
  - PDF 28

## V

- version numbers
  - viewing for products 36
  - viewing with LiveUpdate 36
- viewing
  - latest program update 36
  - versions and dates 36
- virus definitions
  - downloading from Symantec Web site 33
  - file description 10
  - updating with LiveUpdate 33
- viruses
  - alerts 49-53
  - description 10-11
  - how they spread 11
  - in Microsoft Office 10
  - macro viruses 10
  - protection after installation 20
  - repairing infected file 52
  - scanning 16
  - system 10
  - transfer between PC and Macintosh 10
  - Trojan horses 10
  - viewing descriptions 54
  - worms 11

## W

- Web site, Symantec 29, 33
- workstations, protecting 66
- worms 11



# Norton AntiVirus™ for Macintosh®

## CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE. You must be a registered customer in order to receive CD replacements.

If your Symantec product was installed on your computer when you purchased it, contact your hardware manufacturer for CD replacement information.

### FOR CD REPLACEMENT

Please send me: \_\_\_\_\_ CD Replacement

Name \_\_\_\_\_

Company Name \_\_\_\_\_

Street Address (No P.O. Boxes, Please) \_\_\_\_\_

City \_\_\_\_\_ State \_\_\_\_\_ Zip/Postal Code \_\_\_\_\_

Country\* \_\_\_\_\_ Daytime Phone \_\_\_\_\_

Software Purchase Date \_\_\_\_\_

\*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributor.

Briefly describe the problem: \_\_\_\_\_

|                       |                 |  |
|-----------------------|-----------------|--|
| CD Replacement Price  | <u>\$ 10.00</u> | SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%).<br>Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI. |
| Sales Tax (See Table) |                 |  |
| Shipping & Handling   | <u>\$ 9.95</u>  |  |
| TOTAL DUE             | _____           |  |

### FORM OF PAYMENT \*\* (Check One):

\_\_\_\_ Check (Payable to Symantec) Amount Enclosed \$ \_\_\_\_\_ Visa \_\_\_\_\_ Mastercard \_\_\_\_\_ AMEX

Credit Card Number \_\_\_\_\_ Expires \_\_\_\_\_

Name on Card (please print) \_\_\_\_\_ Signature \_\_\_\_\_

\*\*U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.

### MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation  
Attention: Order Processing  
555 International Way  
Springfield, OR 97477 (800) 441-7234  
Please allow 2-3 weeks for delivery within the U.S.

Symantec and Norton AntiVirus are trademarks of Symantec Corporation.  
Other brands and products are trademarks of their respective holder/s.

© 2003 Symantec Corporation. All rights reserved. Printed in the U.S.A.

